Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method for generating a one-way function dependent on a one-way function H and a unique value d for a user, comprising:

holding in memory a function generation unique value s by a right issuer for the user;

creating a value generation unique value u in a unique value calculation unit from the function generation unique value s provided from the memory and the unique value d, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user;

creating by a hash value calculation unit a one-way function value X(M) of a message M by applying the one-way function H to the value generation unique value u from the unique value calculation unit and the message M, where the one-way function value $X(M) = H(u_1 | M) \; | \ldots | \; H(u_m | M)$;

holding a certificate C to prove a public key y paired with the one-way function value X(M);

issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and

verifying the user from the public key y and the capability χ by a right verifier.

2. (Original) The method for generating a one-way function according to claim 1, wherein the value generation unique value u is calculated by applying a one-way function G to the function generation unique value s and the unique value d.

3. (Original) The method for generating a one-way function according to claim 1, wherein the value generation unique value u is calculated by applying an encryption

function E of a symmetric key to the function generation unique value s and the unique value d.

4. (Previously Presented) The method for generating a one-way function according to claim 1, wherein the one-way function value X(M) of the message M is calculated by applying the one-way function H and an encryption function E of a symmetric key to the value generation unique value u and the message M.

5. (Currently Amended) A ~~device~~ computer system that generates ~~for generating~~ one-way function values that calculates a one-way function X dependent on a unique value d for a user, comprising:

means for inputting the unique value d;

means for inputting a message M;

means for holding a function generation unique value s by a right issuer for the user;

means for creating a value generation unique value u from the function generation unique value s from the holding means and the unique value d, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the u-creating means and the message M, where the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$;

means for holding a certificate C to prove a public key y paired with the one-way function value X(M);

means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and means for verifying the user from the public key y and the capability χ.

6. (Currently Amended) The ~~device~~ computer system~~for generating one-way function values~~ according to claim 5, wherein the process of calculating the value generation unique value u and the one-way function value X(M) is difficult to observe from the outside.

7. (Currently Amended) A computer system that performs~~proving device for performing~~ processing based on a private key for a user dependent on a message M, comprising:

means for inputting the message M, the message M including at least identifiers of private key processing algorithms;

means for holding a value generation unique value u for the user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the holding means and the message M;

means for performing processing based on the private key and the one-way function value X(M);

means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and

means for verifying the user from a public key y and the capability χ,

wherein the value generation unique value u is created from a function generation unique value s being held and provided by a right issuer and a unique value d for the user, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user, and the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$; and

wherein the identifiers in the message M enable the private key processing algorithms to be modified.

8. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the calculation process in processing based on the value generation unique value u and the one-way function value X(M) is difficult to observe from the outside.

9. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the ~~proving device~~computer system is configured as one of a small portable operation device ~~such as~~ and a smart card.

10. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the computer system ~~proving device~~ is configured as a module inside a CPU of a computer~~the device~~.

11. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on the private key comprises:

means for inputting a challenge c;

means for calculating a response r from the challenge c and the one-way function value X(M); and

means for outputting the response r.

12. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key comprises:

means for inputting a challenge c;

means for generating a random number k;

means for calculating a response r from the random number k, the challenge c, and the one-way function value X(M); and

means for outputting the response r.

13. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key comprises:

means for generating a random number k;

means for calculating a commitment w from the random number k;

means for inputting a challenge c;

means for calculating the response r from the random number k, the challenge c, and the one-way function value X(M); and

means for outputting the response r.

14. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key comprises:

means for generating a random number k;

means for calculating a commitment w from the random number k;

means for outputting the commitment w;

means for inputting a challenge c;

means for calculating a response r from the random number k, the commitment w, the challenge c, and the one-way function value X(M); and

means for outputting the response r.

15. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key performs multiplications and power operations of multiplicative groups on a finite field.

16. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key performs additions and scalar multiplication operations of elliptic curves on a finite field.

17. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the means for performing processing based on a private key performs multiplicative residue operations and power residue operations modulo n, where n is a composite number that is difficult to factorize.

18. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the message M includes use conditions and the means for inputting messages rejects message input if the use conditions included in the message M are not satisfied.

19. (Currently Amended) The computer system ~~proving device~~ according to claim 7, wherein the message M includes private key processing parameters, and the means for performing processing based on a private key performs processing based on the private key processing parameters included in the message M.

20. (Currently Amended) A ~~device~~ computer system that issues~~for issuing~~ a proving instrument T in accordance with a unique value d for a user, comprising:

means for inputting the unique value d;

means for holding a function generation unique value s by a right issuer for the user;

means for creating a value generation unique value u from the function generation unique value s from the holding means and the unique value d, the value generation unique value u being provided as a series of m values where $u = (u_1,\ldots u_m)$ to a token for the user;

means for writing the value generation unique value u from the u-creating means to the proving instrument T;

means for issuing the proving instrument T that includes a hash function X dependent on the unique value d;

means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and

means for verifying the user from a public key y and the capability χ, wherein the proving instrument T holds the value generation unique value u, and upon input of a message M, creates a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u and the message M to perform processing based on the one-way function value X(M) expressed by $H(u_1 | M) | \ldots | H(u_m | M)$.

21. (Previously Presented) An authentication method by which a right issuer issues rights to right recipients in association with a message M and a right verifier verifies the rights of the right recipients, the method comprising:

creating a value generation unique value u from a function generation unique value s being held and provided by a function generation unique value memory and a unique value d for a user corresponding to the right recipients, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user;

calculating a one-way function value X(M) of the message M by a hash value generator by applying a one-way function H to the value generation unique value u and the message M, where the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$;

issuing a certificate C to prove a public key y paired with the one-way function value X(M) to the right recipients by a certificate issuing unit;

presenting the certificate C from the right recipients to the right verifier;

performing processing by a private key processing unit based on the one-way function value X(M);

verifying the certificate C by a certificate verification unit; and

verifying the processing by a private key processing verification unit based on the one-way function value X(M) of the right recipients with a public key y proved by the certificate C.

22. (Original) The authentication method according to claim 21, wherein an identifier aid indicating an authentication type is included in the certificate C issued by the right issuer and the right verifier succeeds in verifying the certificate C only when the authentication identifier aid included in the certificate C matches the type of authentication to be performed.

23. (Original) The authentication method according to claim 21, wherein use conditions are included in the certificate C issued by the right issuer and the right verifier succeeds in verifying the certificate C only when the use conditions included in the certificate C are satisfied.

24. (Currently Amended) A computer system that issues ~~certificate issuing device for issuing~~ a certificate C in accordance with a unique value d for a user and a message M, comprising:

means for inputting the unique value d;

means for inputting the message M;

means for holding a function generation unique value s by a right issuer for the user;

means for creating a value generation unique value u from the function generation unique value s from the holding means and the unique value d, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the u-creating means and the message M, where the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$;

means for creating a public key y paired with the one-way function value X(M);

means for issuing a certificate C to prove the public key y;

means for issuing a capability χ to the user, the capability χ representing a right of the user in association with the message M; and

means for verifying the user from the public key y and the capability χ.

25. (Currently Amended) A computer system that performs ~~An authentication device for performing~~ authentication in accordance with a message M, comprising:

means for inputting the message M;

means for holding a value generation unique value u for a user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the holding means and the message M;

means for performing processing based on the one-way function value X(M);

means for holding a certificate C to prove a public key y paired with the one-way function value X(M);

means for verifying the certificate C;

means for issuing a capability χ to the user, the capability χ representing a right of the user in association with the message M;

means for verifying the user from the public key y and the capability χ; and

means for verifying processing based on a private key of the user with the public key y,

wherein the value generation unique value u is created from a function generation unique value s being held and provided by a right issuer and the unique value d for the user, the value generation unique value u being provided as a series of m values where u =

$(u_1,\ldots u_m)$ to a token for the user, and where the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$.

26. (Previously Presented) An authentication method by which a right issuer issues rights to right recipients in association with a message M and a right verifier verifies the rights of the right recipients, the method comprising:

creating a value generation unique value u from a function generation unique value s being held and provided by a function generation unique value memory and a unique value d for a user corresponding to the right recipients, the value generation unique value u being provided as a series of m values where $u = (u_1,\ldots u_m)$ to corresponding tokens for the right recipients;

calculating a one-way function value X(M) of the message M by a hash value generator by applying a one-way function H to the value generation unique value u from the right issuer and the message M;

issuing an access ticket t by an access ticket issuing unit determined from a private key x and the one-way function value X(M) to the right recipients, where $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$;

performing processing by a private key processing unit based on the one-way function value X(M);

converting the processing by a private key processing conversion unit based on the one-way function value X(M) to the processing based on the private key x by the access ticket t; and

verifying the processing by a private key processing verification unit based on the one-way function value X(M) of the right recipients with a public key y paired with the private key x by the right verifier.

27. (Original) The authentication method according to claim 21, wherein an identifier aid indicating an authentication type is included in the message M.

28. (Currently Amended) A computer system that issues~~An access ticket issuing device for issuing~~ an access ticket in accordance with a unique value d for a user and a message M, comprising:

means for inputting the unique value d;

means for inputting the message M;

means for holding a function generation unique value s by a right issuer for the user;

means for creating a value generation unique value u from the function generation unique value s from the holding means and the unique value d, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u and the message M, where the one-way function value $X(M) = H(u_1 | M) \; | \ldots | \; H(u_m | M)$;

means for creating the access ticket t from a private key x and the one-way function value X(M);

means for issuing the access ticket t;

means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M; and

means for verifying the user from a public key y and the capability χ.

29. (Currently Amended) ~~The access ticket issuing device~~The computer system according to claim 28, wherein the access ticket t is calculated as a difference (x – X(M)) between the private key x and the one-way function value X(M).

30. (Currently Amended) The computer system ~~The access ticket issuing device~~ according to claim 28, wherein the access ticket t is calculated as a quotient x/X(M) between the private key x and the one-way function value X(M).

31. (Currently Amended) The computer system ~~The access ticket generation device~~ according to claim 28, wherein the unique value d for the user is $(d_1,\ldots,d_m)$, the value generation unique value u is $(u_1,\ldots,u_m)$ and the one-way function value X(M) is generated from bit concatenation $H(u_1 | M) | \ldots | H(u_m | M)$ of the value of the one-way function H and has a desired bit length.

32. (Currently Amended) The computer system ~~The access ticket generation device~~ according to claim 31, wherein the value generation unique value $(u_1,\ldots,u_m)$ is found from $u_j=G(s_j | d)$ obtained by applying a one-way function G to the function generation unique value $s = (s_1,\ldots,s_m)$.

33. (Currently Amended) A computer system that performs ~~An authentication device for performing~~ authentication for a user in accordance with a message M, comprising:

means for inputting the message M;

means for holding a value generation unique value u for the user;

means for creating a one-way function value X(M) of the message M by applying a one-way function H to the value generation unique value u from the holding means and the message M;

means for performing processing based on the one-way function value X(M);

means for holding an access ticket t determined from a private key x and the one-way function value X(M);

means for converting the processing based on the one-way function value X(M) to processing based on the private key x by the access ticket t;

means for holding a public key y paired with the private key x;

means for issuing a capability χ from the right issuer to the user, the capability χ representing a right of the user in association with the message M;

means for verifying the user from the public key y and the capability χ; and

means for verifying the processing based on the private key x with the public key y,

wherein the value generation unique value u is created from a function generation unique value s being held and provided by a right issuer and a unique value d provided for the user, the value generation unique value u being provided as a series of m values where $u = (u_1, \ldots u_m)$ to a token for the user, and where the one-way function value $X(M) = H(u_1 | M) | \ldots | H(u_m | M)$.

34. (Currently Amended) The ~~authentication device~~computer system according to claim 33, wherein the means for converting the processing based on the private key comprises means for updating a challenge c with the access ticket t.

35. (Currently Amended) The computer system ~~authentication device~~ according to claim 33, wherein the means for converting the processing based on the private key comprises means for updating a response r with the access ticket t.

36. (Currently Amended) The computer system ~~authentication device~~ according to claim 33, wherein the means for converting the processing based on the private key comprises means for updating a response r with the access ticket t and a challenge c.

37. (Currently Amended) The computer system ~~authentication device~~ according to claim 33, wherein the means for converting the processing based on the private key comprises means for updating a challenge c with a commitment w and means for updating a response r with the access ticket t and the challenge c.

38. (Currently Amended) The computer system ~~authentication device~~ according to claim 33, wherein the means for converting the processing based on the private key comprises

means for updating a challenge c with the access ticket t and a commitment w, and means for updating a response r with the commitment w.